UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/817,124	04/02/2004	Glenn A. Morten	08223/1200330-US2	1508

7278 7590 11/26/2008

DARBY & DARBY P.C.
P.O. BOX 770
Church Street Station
New York, NY 10008-0770

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	**PAPER NUMBER**
2436	

MAIL DATE	DELIVERY MODE
11/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/817,124	MORTEN ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application amendments filed on **9-4-2008**.

2. Claims **21 - 28** are pending. Claims **21 - 28** are new. Claims **1 - 20** have been cancelled. Claims **21, 26, 28** are independent. This application was filed on **4-2-2004**.

Response to Arguments

3. Applicant's arguments filed 3-12-2008 have been fully considered but they are not persuasive.

Responses:

Applicant's invention is principally encryption of content to provide a measure of protection against unauthorized access. Applicant's invention uses a mixture of encryption and the application of watermark technology in order to protect the content. The watermark attached to the content must be identifiable for the entity that attached the watermark. The entity in this case is the market participant or downstream media content reseller. And, Applicant's invention discloses the capability to place multiple watermarks upon a single piece of media content. These functions are disclosed by the referenced prior art.

A reseller for media content is no different than the original content owner who watermarks his/or her media content to uniquely identify the content as belonging to the media content owner. Cooper discloses a media content distributor (reseller, original

content owner). The media content is watermarked before it is transferred to a user as per claimed invention. (see Cooper paragraph [0037], lines 1-3; paragraph [0019], lines 5-9; paragraph [0198], lines 8-19: content is transferred to a user; content distributor)

Applicant's invention appears to be the ability to watermark content with a watermark that is uniquely identifiable to a specific individual or entity and the placement of multiple watermarks if necessary onto a piece of media content. Cooper discloses that a watermark is placed upon content that uniquely identifies the entity that watermarks the content. (see Cooper paragraph [0196], lines 1-7: unique identifier for media content and where it came from (distributor)) This feature is disclosed by the referenced prior art.

The Cooper prior art discloses the concept and capability of a content distributor. And, Cooper discloses the ability to watermark content, encrypt media content and download the media content to a user. These actions are the same actions outlined in claim 1. Take (received) media content, place a unique watermark upon content, encrypt, and distribute the encrypted content. (see Cooper paragraph [0198], lines 8-19: watermark and encrypt content) And, Cooper discloses the placement of multiple watermarks onto media content. (see Cooper paragraph [0249], lines 1-15: multiple watermarks)

There is no indication that this must not be accomplished by using a certificate authority or any other certificate related mechanism. In any event, Cooper prior art discloses an ability to place a watermark onto media content that uniquely identifies an

entity. (see Cooper paragraph [0196], lines 1-7: watermark, unique identification where content came from)

The Cooper prior art discloses a content distributor. (see Cooper paragraph [0196], lines 1-7: unique identifier for media content and where it came from (distributor); paragraph [0198], lines 8-19; encrypt content, customer ID may also be added as an additional watermark)

The Cooper prior art discloses the capability for multiple watermarks to be place onto a media content and the capability for encryption of the media content after watermark(s) placement. (see Cooper paragraph [0249], lines 1-15: multiple watermarks placed onto media content) This satisfies the functions of multiple watermarks for a piece of media content.

Claim Objections

4. Claim **22** is objected to because of the following informalities:

Claim **22** is dependent on Claim **22**. Claim cannot depend on itself. Examiner interpreted Claim **22** as dependent on Claim **21** for this action. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims **21 - 28** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

For Claims **21 - 23, 25 - 28**, there is no disclosure for "a plurality of network devices". The term, "network devices" is not disclosed in the specification or the original claims. The specification discloses a network device and a distributed network. A distributed network implies that all of the processing functions of a network device are spread across several network-connected nodes. (see specification page 6, lines 25-26) Not, that all the functions of a network device are duplicated across each network device in the network.

For Claim **24**, there is no disclosure for: "at least one of a serial number, and a time stamp indicating approximately when the content is decrypted". The specification discloses that the timestamp represents when the wrapper was created not when the content was decrypted. (see specification page 15, lines 2-3: "The identifier may also include a time stamp representing when the wrapper is created.". This disclosure indicates the timestamp represents the time when the wrapper is created not when the content is decrypted. This is the only disclosure for the term "timestamp" in the specification.

For Claim **22**, there is no disclosure for: “absent decrypting the received encrypted content“. The term “absent” is not disclosed in the specification of the original claims.

Appropriate corrections are required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims **21 - 25, 27, 28** are rejected under 35 U.S.C. 102(e) as being anticipated by **Benaloh et al.** (US Patent No. **7,065,216**).

Regarding Claim 21, Benaloh discloses a system for tracing content in a highly distributed system, comprising:

a plurality of network devices, wherein each network device in the plurality is configured to perform actions, comprising:

b) receiving encrypted content associated with a content owner in the highly distributed system; (see Benaloh col. 1, lines 63-66: content received (provided); col. 12, lines 10-14: network (distributed) access to content; there is no disclosure for "a plurality of network devices")

b) determining if the received content is to be decrypted; (see Benaloh col. 6, lines 4-7: use the key to decrypt and play the encrypted movie; (content decryption required for playback))

if the received content is to be decrypted:

c) decrypting the received content, (see Benaloh col. 2, lines 8-10: content decrypted)

determining a self-identifier that uniquely identities the current network device in the plurality of network devices, and modifying the decrypted content by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

if the decrypted content is to be provided to another network device in the plurality of network devices:

d) encrypting the modified content; (see Benaloh col. 10, lines 6-10: encrypt contents)

e) wrapping the encrypted modified content together with the self-identifier using an access key; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

f) providing the wrapped encrypted modified content to the other network device in the plurality of network devices. (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14: transfer encrypted content to end user, downstream market recipient)

Regarding Claim 22, Benaloh discloses the system of claim 21, wherein each network device in the plurality of network devices is further configured to perform action, further comprising: if the received encrypted content is to be provided to another network device in the plurality of network devices absent decrypting the received encrypted content, providing the received encrypted content to the other network device in the plurality of the network devices. (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14: transfer encrypted content to end user, downstream market recipient; there is no disclosure for: “absent decrypting the received encrypted content”)

Regarding Claim 23, Benaloh discloses the system of claim 22, wherein decrypting the received encrypted content further comprises:

a) obtaining a different access key out-of-band, wherein the different access key is uniquely associated with the network device currently having decrypted the content and a sending network device of the content to the current network device in the plurality of network devices; (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14; col. 6, lines19-23: receive content (access) key (network, other); there is no disclosure of different access keys) and

b) employing the different access key to unwrap the received content before decrypting the received content. (see Benaloh col. 10, lines 16-19: decrypt content using access key; there is no disclosure of different access keys)

Regarding Claim 24, Benaloh discloses the system of claim 22, wherein the self-identifier further comprises at least one of a serial number, and a time stamp indicating approximately when the content is decrypted. (see Benaloh col. 6, lines 25-27: serial number, identify content player; no disclosure for : "at least one of a serial number, and a time stamp indicating approximately when the content is decrypted")

Regarding Claim 25, Benaloh discloses the system of claim 22, wherein the set of information further comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the current network device in the plurality of network devices. (see Benaloh col. 2, lines 36-39: traceability information)

Regarding Claim 27, Benaloh discloses the network device in a plurality of network devices of Claim 26, wherein at least one of the network devices is managed by at least one of a content owner, a content aggregator, a service operator, or an end-user. (see Benaloh col. 4, line 66 - col. 5, line 5: content provider(s), aggregator)

Regarding Claim 28, Benaloh discloses a method for tracing content in a highly distributed system, comprising: for each network device in a plurality of network devices along the highly distributed system:

a) receiving encrypted content by a current network device in the plurality of network devices in the highly distributed system; (see Benaloh col. 1, lines 63-66:

content received (provided); col. 12, lines 10-14: network (distributed) access to content)

b) determining if the received content is to be decrypted, (see Benaloh col. 6, lines 4-7: use the key to decrypt and play the encrypted movie; (content decryption required for playback)) and

if the received content is to be decrypted:

c) decrypting the received content, (see Benaloh col. 2, lines 8-10: content decrypted)

d) determining a self-identifier that uniquely identities the current network device in the plurality of network devices, (see Benaloh col. 6, lines 25-27: serial number, identifier for content player) and

e) modifying the decrypted content by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier for the current network device; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

if the decrypted content is to be provided to another network device in the plurality of network devices:

f) encrypting the modified content; (see Benaloh col. 10, lines 6-10: encrypt contents)

g) wrapping the encrypted modified content together with the self-identifier using an access key; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

h) providing the encrypted modified content to the other network device in the plurality of network devices. (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14: transfer encrypted content to end user, downstream market recipient)

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim **26** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Benaloh** in view of **Cooper et al.** (US PGPUB No. **20010051996**).

Regarding Claim 26, Benaloh discloses a network device in a plurality of network devices for managing content in a highly distributed system, wherein each network device comprises:

a) arranged to receive and to send content to another network device in the plurality of network devices; (see Benaloh col. 1, lines 63-66: content received (provided); col. 12, lines 10-14: network (distributed) access to content) and

b) configured to execute program code that performs actions, including: receiving encrypted content in the highly distributed system; (see Benaloh col. 1, lines 63-66: content received (provided); col. 12, lines 10-14: network (distributed) access to content; col. 4, lines 18-20; col. 4, lines 32-37: software, implementation means)

c) determining if the received content is to be decrypted, and if the received content is to be decrypted: decrypting the received content, (see Benaloh col. 2, lines 8-10: content decrypted)

d) determining a self-identifier that uniquely identities the current network device in the plurality of network devices (see Benaloh col. 6, lines 25-27: serial number, identifier for content player), and modifying the decrypted content by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

if the decrypted content is to be provided to another network device in the plurality of network devices:

e) encrypting the modified content; (see Benaloh col. 10, lines 6-10: encrypt contents)

f) wrapping the encrypted modified content together with the self-identifier using an access key; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

g) providing the encrypted modified content to the other network device in the plurality of network devices. (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14: transfer encrypted content to end user, downstream market recipient)

Benaloh does not specifically disclose a transceiver and a processor. However, Cooper discloses a transceiver and a processor. (see Cooper paragraph [0039], lines 12-16: network communications device such as a network interface card (transceiver); see specification page 8, line 5))

It would have been obvious to one of ordinary skill in the art to modify Benaloh for a transceiver and a processor as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13: " … Therefore, there is a need in the electronic media content distribution field to be able to mark content files with an authenticated digital signature that uniquely identifies the person who is the source, to be able to monitor the files if they are transferred to others, and to have these capabilities while imposing minimal burden and inconvenience on the consumer. … ")

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2436
11/24/2008

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
November 10, 2008